

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

REC'D 23 FEB 2006

WIPO

PCT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 10.289/K	FOR FURTHER ACTION	
See Form PCT/IPEA/416		
International application No. PCT/HU2004/000101	International filing date (day/month/year) 02.11.2004	Priority date (day/month/year) 01.03.2004
International Patent Classification (IPC) or national classification and IPC H04L29/06, H04M1/253		
Applicant JOBBAGY, Miklos		
<p>1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of 5 sheets, including this cover sheet.</p> <p>3. This report is also accompanied by ANNEXES, comprising:</p> <p>a. <input checked="" type="checkbox"/> <i>(sent to the applicant and to the International Bureau) a total of 15 sheets, as follows:</i></p> <p><input checked="" type="checkbox"/> sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).</p> <p><input type="checkbox"/> sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.</p> <p>b. <input type="checkbox"/> <i>(sent to the International Bureau only) a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).</i></p>		
<p>4. This report contains indications relating to the following items:</p> <p><input checked="" type="checkbox"/> Box No. I Basis of the opinion</p> <p><input type="checkbox"/> Box No. II Priority</p> <p><input type="checkbox"/> Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p><input type="checkbox"/> Box No. IV Lack of unity of invention</p> <p><input checked="" type="checkbox"/> Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p><input type="checkbox"/> Box No. VI Certain documents cited</p> <p><input type="checkbox"/> Box No. VII Certain defects in the international application</p> <p><input type="checkbox"/> Box No. VIII Certain observations on the international application</p>		
Date of submission of the demand 28.09.2005	Date of completion of this report 22.02.2006	
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Horn, M.P. Telephone No. +49 89 2399-7579	



INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/HU2004/000101

Box No. I Basis of the report

1. With regard to the **language**, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.
 - This report is based on translations from the original language into the following language, which is the language of a translation furnished for the purposes of:
 - international search (under Rules 12.3 and 23.1(b))
 - publication of the international application (under Rule 12.4)
 - international preliminary examination (under Rules 55.2 and/or 55.3)
2. With regard to the **elements*** of the international application, this report is based on (replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report):

Description, Pages

1-13 filed with the demand

Claims, Numbers

1-3 filed with the demand

Drawings, Sheets

1 as originally filed

- a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing

3. The amendments have resulted in the cancellation of:
 - the description, pages
 - the claims, Nos. 4
 - the drawings, sheets/figs
 - the sequence listing (specify):
 - any table(s) related to sequence listing (specify):
4. This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).
 - the description, pages
 - the claims, Nos.
 - the drawings, sheets/figs
 - the sequence listing (specify):
 - any table(s) related to sequence listing (specify):

* If item 4 applies, some or all of these sheets may be marked "superseded."

**INTERNATIONAL PRELIMINARY REPORT
ON PATENTABILITY**

International application No.
PCT/HU2004/000101

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	1-3
	No: Claims	
Inventive step (IS)	Yes: Claims	1-3
	No: Claims	
Industrial applicability (IA)	Yes: Claims	1-3
	No: Claims	

2. Citations and explanations (Rule 70.7):

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following document:

D1: EP-A-1 328 101 (AVAYA TECHNOLOGY CORP) 16 July 2003 (2003-07-16)

2 The document D1 is regarded as being the closest prior art to the subject-matter of claim 1. It discloses:

2.1 Set of equipment for secure direct information transfer over the Internet, which contains information transmitting terminal devices suitable for collaborating with an information forwarding network, taking part in the information traffic, the individual information transmitting terminal devices are equipped with a sender partial unit, a receiver partial unit and a storage partial unit comprising an ID-register containing a device identification signal, a C-register suitable for storing a coding key and a D-register suitable for storing a decoding key, where the C-register containing the coding key is in connection with the sender partial unit, and a coding key and a collaborating decoding key are allocated to the individual information transmitting terminal devices, the storage partial unit of each information transmitting terminal device is completed with one or more temporary storage registers for the temporary storage of the coding keys of other information transmitting terminal devices, while the information forwarding network is completed with at least one central traffic co-ordinating unit, the central traffic coordinating unit has an MD-register storing a master decoding key and a memory unit containing base cells for storing the coding keys belonging to the individual information transmitting terminal devices and a master coding key collaborating with the master decoding key is allocated to the central traffic co-ordinating unit, and the C-registers of the information transmitting terminal devices are provided with a master coding key collaborating with the master decoding key stored in the MD-register of the central traffic co-ordinating unit,

2.2 The subject-matter of claim 1 differs mainly from the disclosure of document D1 in that:

**INTERNATIONAL PRELIMINARY
REPORT ON PATENTABILITY
(SEPARATE SHEET)**

International application No.
PCT/HU2004/000101

In the storage partial unit of the individual information transmitting terminal devices there is only information free from the given information transmitting terminal device's own coding key, while only the coding key of the other information transmitting terminal device participating in the information exchange is temporarily stored in the temporary storage register of the first information transmitting terminal device, and only the coding key of the first information transmitting terminal device participating in the information exchange is temporarily stored in the temporary storage register of the other information transmitting terminal device.

The subject-matter of claim 1 is therefore new (Article 33(2) PCT).

- 2.3 The problem to be solved by the present invention is to increase the security of the encrypted communication session.
- 2.4 The solution to this problem proposed in claim 1 of the present application is considered as involving an inventive step (Article 33(3) PCT) for the following reasons:

Document D1 does neither disclose nor suggest the use of independent coding and decoding keys for a communication session between two communicating parties. Moreover, document D1 does neither disclose nor suggest that the parties are unaware of their respective coding key.

In fact, document D1 teaches away from such a solution because it discloses the encryption of the communication session by a single session key which is effectively chosen by the calling party.

The other prior-art cited in the search report does not relate to individual coding and decoding keys but also to a single session key.

- 2.5 Claims 2 and 3 are dependent on claim 1 and as such also meet the requirements of the PCT with respect to novelty and inventive step.

Set of equipment for secure direct information transfer over the Internet

The subject of the invention is a set of equipment for secure direct information transfer over the Internet, which contains information transmitting terminal devices suitable for collaborating with an information forwarding network, taking part in the information traffic, the individual information transmitting terminal devices are equipped with a sender partial unit, a receiver partial unit and a storage partial unit comprising an ID-register containing a device identification signal, a C-register suitable for storing a coding key and a D-register suitable for storing a decoding key, where the C-register containing the coding key is in connection with the sender partial unit, and a coding key and a collaborating decoding key are allocated to the individual information transmitting terminal devices, the storage partial unit of each information transmitting terminal device is completed with one or more temporary storage registers for the temporary storage of the coding keys of other information transmitting terminal devices, while the information forwarding network is completed with at least one central traffic co-ordinating unit, the central traffic co-ordinating unit has an MD-register storing a master decoding key and a memory unit containing base cells for storing the coding keys belonging to the individual information transmitting terminal devices and a master coding key collaborating with the master decoding key is allocated to the central traffic co-ordinating unit, and the C-registers of the information transmitting terminal devices are provided with a master coding key collaborating with the master decoding key stored in the MD-register of the central traffic co-ordinating unit.

Due to technical development, especially the development of computer technology and telecommunication electronic equipment are becoming widely used, with the help of which sound and other signal transmission solutions can be realised. In some of these solutions not the ordinary public telecommunication networks are used, and in certain cases, e.g.: for transmitting bank information and making transactions, the transmitted data is coded or encrypted.

International patent No. WO 00/41383 describes a solution with the help of which, in the case that there is appropriate private branch exchange between two telephone sets, the communication chain can be established in a way that after initiating a call first the control unit of the branch exchange finds a remote access database indexing telephone numbers and Internet addresses, there it tries to find the called number, and if it can identify it, then reading the Internet address belonging to the telephone number it establishes the telephone call over the Internet rather than over the public telephone network, and if it does not find such a telephone number – Internet identifying connection, then it establishes the telephone call over the ordinary public telephone network.

However, the disadvantage of the solution is that if there is no Internet access to the dialled telephone number, then the connection is established in the ordinary way, over the public telephone network, which always results in extra costs for the calling party.

A further disadvantage is that for a cost friendly solution, beside the Internet accessibility of the calling and the called party, traditional telephone connection is also needed, and even individual special private branch exchanges need to be established, which results in a significant increase of the investment costs and also requires further operation and maintenance expenses.

Another significant disadvantage of the solution is that the encryption of the data traffic connection is not solved, and so the traffic can be tapped, it is easily accessible for unauthorised third parties, and by this the established signal forwarding line cannot be used for transmitting optional data.

Another solution is described in international patent application No. WO99/62222 relates to the encryption of telephone traffic. Its main point is that the individual users are given their own password, which they must enter for the central unit in every case after they log in, for the purpose of identifying themselves. The identified users are provided with limited access time from the central unit, during which time their data traffic is encrypted.

However, the greatest disadvantage of this solution is that the period of encrypted data traffic is restricted in time, which in the case when longer connection is needed excludes the possibility of confidential information transfer.

A further disadvantage is that in this case the users must log in the system themselves, and then they must send the central unit a password, which was given to them, so other parties may also know it, and because of the possibility of using a password accessible to other parties confidential data traffic becomes uncertain, and it becomes questionable whether this channel can be used exclusively by a given device or user.

Patent document EP 1.328.101 is also known, this presents a set of equipment that realises coded information transfer with the combination of centralised communication networks similar to the traditional telephone system and the TAN number system known in the financial sphere.

The disadvantage of this solution is that it uses a single key algorithm for the coding of the communication, and it stores all the keys for this in a single place, in the call complex. In this way the system is vulnerable via the call complex, all the communication taking place in the network can be decoded from inside the call complex or while in the possession of the call complex or its data.

Another significant disadvantage of this solution is that the symmetrical keys needed for the decoding of the encrypted communication are required to travel continuously between the elements of the network, and so they can be obtained resulting in the encrypted messages becoming decidable for unauthorised persons, which is inadmissible from the point of view of the system.

A further disadvantage of the solution is that all communication takes place through the call complex, so the data transfer capacity of the call complex is continually burdened in proportion with the number of communications taking place at any specific point in time.

On the basis of the above our aim with the invention was to overcome the deficiencies of the known solutions and to create a set of equipment with the help of which a

connection realising sound, signal or other data traffic can be established in a way identical to ordinary telephoning, so that encrypted information traffic becomes possible independently from the time needed for the connection, during its complete period, and such use always takes place over the Internet, avoiding the public telephone network, which always involves using costs.

The idea behind the invention is based on the recognition that if a suitably constructed central computer unit and terminal devices suitable for establishing Internet-based connection are provided with coding and decoding keys in a way different from the known solutions, then a situation can be achieved where Internet-based communication can be realised in the course of which the sound, still picture, moving picture, signal or other data traffic between the calling party and the called party in connection with each other takes place in an encrypted way impossible to disassemble from the time when the connection is established until it is ended, so that the users of the system do not have any encryption keys or passwords that could be appropriated and by this could endanger the integrity of the network, furthermore the central computer unit in itself is suitable for controlling and managing communication between the terminal devices, and so the task can be solved.

In accordance with the set aim the set of equipment according to the invention for secure direct information transfer over the Internet, – which contains information transmitting terminal devices suitable for collaborating with an information forwarding network, taking part in the information traffic, the individual information transmitting terminal devices are equipped with a sender partial unit, a receiver partial unit and a storage partial unit comprising an ID-register containing a device identification signal, a C-register suitable for storing a coding key and a D-register suitable for storing a decoding key, where the C-register containing the coding key is in connection with the sender partial unit, and a coding key and a collaborating decoding key are allocated to the individual information transmitting terminal devices, the storage partial unit of each information transmitting terminal device is completed with one or more temporary storage registers for the temporary storage of the coding keys of other information transmitting terminal devices, while the information forwarding network is completed with at least one central traffic co-ordinating unit, the central traffic co-ordinating unit has an MD-register storing a master

decoding key and a memory unit containing base cells for storing the coding keys belonging to the individual information transmitting terminal devices and a master coding key collaborating with the master decoding key is allocated to the central traffic co-ordinating unit, and the C-registers of the information transmitting terminal devices are provided with a master coding key collaborating with the master decoding key stored in the MD-register of the central traffic co-ordinating unit – is constructed in a way that in the storage partial unit of the individual information transmitting terminal devices there is only information free from the given information transmitting terminal device's own coding key, while only the coding key of the other information transmitting terminal device participating in the information exchange is temporarily stored in the temporary storage register of the first information transmitting terminal device, and only the coding key of the first information transmitting terminal device participating in the information exchange is temporarily stored in the temporary storage register of the other information transmitting terminal device, and so for the duration of the actual information exchange the first information transmitting terminal device and the other information transmitting terminal device are directly linked to one another permitting data flow without the mediation of the central traffic co-ordinating unit.

A further criterion of the set of equipment according to the invention may be that the temporary storage registers of the information transmitting terminal devices are connected to the sender partial unit.

In the case of a possible construction of the set of equipment the central traffic co-ordinating unit is provided with an MC-register storing a master coding key.

In another different realisation of the invention in the storage partial unit of the individual information transmitting terminal devices there is only information free from the given information transmitting terminal device's own coding key.

The greatest advantage of the set of equipment according to the invention is that with its use connection between the calling party and the called party can be established with simple means, as in the case of ordinary telephone use, but the costs of information flow

are significantly lower, while it is guaranteed that the flow of data remains encrypted during the complete period of the connection.

It must also be regarded as an advantage that due to the information transmitting terminal device belonging to the set of equipment no further expensive additional elements need to be acquired, operated or maintained, which has a favourable influence on the expenses in connection with the use of the equipment.

It must also be regarded as an advantage that the specially constructed information transmitting terminal device itself, together with the central traffic co-ordinating unit, realises the encrypting of the data traffic, and so there is no need for a code, identifier or other additional key given to the users, also accessible to unauthorised parties. Another advantage deriving from this is that it cannot happen that the users cannot enter the system, because they forgot their own code.

A further favourable characteristic of the invention is that the data traffic between the two end points does not take place through a central exchange, which accelerates the flow of information and improves the security of the system, makes the data impossible to disassemble and makes the system impossible to tap.

It is also a disadvantage that as a result of the special nature of the set of equipment according to the invention the terminal devices are impossible to use, if the central computer unit is avoided, which results in that the users of the terminal devices can enter the system only with the approval of the operator of the central computer unit.

A further advantage is that the set of equipment can be installed independently from the manufacturer so that the terminal devices and the central computer unit is uploaded with key pairs by a given operator, and so a closed network can be created, which makes communication possible only for a certain group of users.

Below the set of equipment according to the invention is described in detail in connection of a construction example, on the basis of a drawing. In the drawing

Figure 1 shows a schematic picture of the arrangement of the set of equipment according to the invention.

Figure 1 shows a version of the set of equipment according to the invention, in the case of which – for the sake of simplicity – only one call initiating information transmitting terminal device 10 and one call receiving information transmitting terminal device 20 is detailed. However, it is clear that the set of equipment can contain an optional number of information transmitting terminal devices 10. The number of information transmitting terminal devices is only restricted by the capacity of the central traffic co-ordinating unit 40.

Connection between the information transmitting terminal device 10 and the information transmitting terminal device 20 is established by the information forwarding network 30, with the help of the central traffic co-ordinating unit 40. The information forwarding network 30 can be an optional communication network, which in this case can mean a wired or wireless, private or public network. The only requirement with respect to the information forwarding network 30 is that it should be suitable for transmitting the signals to be forwarded at a high data rate used in telecommunication, possibly free from distortion.

It can be seen in figure 1 that the central traffic co-ordinating unit 40 is a high-capacity computer device, which has an MC-register 41 and an MD-register 42 on the one part and contains a memory unit 43 on the other part. In the MC-register 41 there is a master coding key 41a, while in the MD-register 42 there is a master decoding key 42a. This unique key-pair enables the information transmitting terminal device 10 and the information transmitting terminal device 20 to realise encrypted data traffic with the central traffic co-ordinating unit 40. In the memory unit 43 of the central traffic co-ordinating unit 40 there is a base cell 43a and another base cell 43b, in which the coding key 16 of the information transmitting terminal device 10 and the coding key 26 of the information transmitting terminal device 20 can be found in a resident way.

However, it must be pointed out here that the master coding key 41a and the MC-register 41 containing it 41 does not necessarily have to be situated in the central traffic co-

ordinating unit 40. The MC-register and the master coding key 41a can be situated remote from the central traffic co-ordinating unit so that the master coding key 41a and the master decoding key 42a are not accessible on the same place.

Similarly to traditional telephone sets the information transmitting terminal device 10 has a keyboard, microphone and sound emitter – not shown here – and apart from these it also has a storage partial unit 11, a sender partial unit 18 and a receiver partial unit 19. The storage partial unit 11 also has an ID-register 12 for recording the device identification signal 12a and a D-register 14 containing the information transmitting terminal device's 10 own decoding key 17. The C-register 13 suitable for the temporary or permanent storage of the master coding key 41a of the central traffic co-ordinating unit 40 also belongs here, as well as the temporary storage register 15, which is responsible for storing the coding key 26 of the other terminal device performing actual data traffic – in our case this is the information transmitting terminal device 20 – during the connection. Practically the temporary storage register 15 of the information transmitting terminal device 10 should be connected to the sender partial unit 18.

Practically the structural construction of the information transmitting terminal device 20 is the same as that of the information transmitting terminal device 10. Similarly to traditional telephone sets it also has a keyboard, microphone and sound emitter – not shown here either – and a storage partial unit 21, a sender partial unit 28 and a receiver partial unit 29. The ID-register 22, the D-register 24 and the temporary storage register 25 belong to the storage partial unit 21. The ID-register records the unique device identifying signal 22a of the information transmitting terminal device 20, while the D-register 24 carries the information transmitting terminal device's 20 own decoding key 27. The coding key 16 of the currently connected information transmitting terminal device 10 – in our case – can be found in the temporary storage register 25. And in this case too the C-register 23 is for the temporary or permanent storage of the master coding key 41a. From the aspect of the information transmitting terminal device 20 it is favourable, if the temporary storage register 25 is in connection with the sender register 28.

In the course of a possible realisation of the operation of the set of equipment the information transmitting terminal device 10 acts as the call initiating unit, and the information transmitting terminal device 20 acts as the called unit, but the set of equipment is also suitable for establishing several signal forwarding connections simultaneously, that is for establishing so-called conference connection.

Dialling the unique identifying number, e.g.: telephone number, of the information transmitting terminal device 20 or the device identifying signal 22a of the information transmitting terminal device 20 on the information transmitting terminal device 10, it sends its login through the information forwarding network to the central traffic co-ordinating unit 40 in a way that the information transmitting terminal device 10 codes the login message with the help of the master coding key 41a situated in the C-register 13 of the information transmitting terminal device, and it furthers the coded signal through the sender partial unit 18 to the central traffic co-ordinating unit 40.

With the help of the master decoding key 42a recorded in its MD-register 42 the central traffic co-ordinating unit 40 disassembles the message coded with the master coding key 41a. On the one part on the basis of the content of the message it identifies the information transmitting terminal device 10 on the basis of its own device identifying signal 12a, and on the other part it checks whether an information transmitting terminal device 20 really belongs to the received device identifying signal 22a, and if yes, according to the device identifying signal 22a it finds the coding key 26 of the information transmitting terminal device 20 in the base cell 43b of the memory unit 43. The central traffic co-ordinating unit 40 encrypts the coding key 26 of the information transmitting terminal device 20 with the help of the coding key 16 of the information transmitting terminal device 10 and sends it to the receiver partial unit 19 of the information transmitting terminal device 10. The receiver partial unit 19 of the information transmitting terminal device 10 disassembles the received information with the help of its decoding key 17 and by this it gains temporary access to the coding key 26 of the information transmitting terminal device, which it stores in the temporary storage register 15 of the information transmitting terminal device.

The call initiating information transmitting terminal device 10 tries to get in contact with the information transmitting terminal device 20 through the information forwarding network 30. If the information transmitting terminal device 10 cannot get in contact with the information transmitting terminal device 20 belonging to the device identifying signal 22a, then the connection cannot be established.

In the case that the information transmitting terminal device 10 has managed to get in contact with the information transmitting terminal device 20, then it sends its own device identifying signal 12a encrypted with the coding key 26 of the information transmitting terminal device 10 to the information transmitting terminal device 20. The information transmitting terminal device 20 disassembles it with its own decoding key 27 and then coding it with the help of the master coding key belonging to the central traffic co-ordinating unit 40 it sends it through the information forwarding network 30 to the central traffic co-ordinating unit 40, and requests the coding key 16 of the information transmitting terminal device 10 from it.

In accordance with the device identifying signal 12a received from the information transmitting terminal device 20 the central traffic co-ordinating unit 40 selects the coding key 16 of the information transmitting terminal device from the base cell 43a of the memory unit 43. Then the central traffic co-ordinating unit 40 encrypts the coding key 16 of the information transmitting terminal device 10 with the help of the coding key 26 of the information transmitting terminal device 20, and sends it to the information transmitting terminal device 20. The information transmitting terminal device 20 receives the encrypted message sent by the central traffic co-ordinating unit 40 in its receiver partial unit 29, disassembles it with its own decoding key 27 as a result of which it gets to know the coding key 16 of the call initiating information transmitting terminal device 10, which it stores temporarily in the temporary storage register 25 of the information transmitting terminal device 20 in a way impossible to read.

After the coding key 16 has been sent to the information transmitting terminal device 20 and the coding key 26 has been sent to the information transmitting terminal device 10 the information transmitting terminal device 10 can encrypt its information to be sent to the

information transmitting terminal device 20 with the help of the coding key 26, so that now the information can be sent through the sender partial unit 18 straight to the information transmitting terminal device 20, which in its receiver partial unit 29 receives the data sent from the sender partial unit 18 of the information transmitting terminal device 10 through the information forwarding network 30 – and coded with the coding key 26 of the information transmitting terminal device 20 – it can disassemble it and so it becomes easily interpretable for the person or equipment using the information transmitting terminal device 20.

The information transmitting terminal device 20 can answer the information received from the information transmitting terminal device 10 so that it encrypts the data it intends to send with the help of the coding key 16 situated in the temporary storage register 25, sends it to the sender partial unit 28, from there to the information forwarding network 30, and then it is directly furthered to the receiver partial unit 19 of the information transmitting terminal device 10. It tries to disassemble the data arriving at the receiver partial unit 19 with the decoding key 17 of the information transmitting terminal device 10, and it succeeds, then the data can be easily interpreted by the person or equipment using the information transmitting terminal device 10.

This direct signal traffic between the information transmitting terminal device 10 and the information transmitting terminal device 20 through the information forwarding network is realised in a way that the central traffic co-ordinating unit 40 does not take part in it. The information transmitting terminal device 10 and the information transmitting terminal device 20 temporarily get to know each other's coding key 16 and coding key 26, and they are able to realise direct information exchange. After the termination of the traffic between information transmitting terminal device 10 and the information transmitting terminal device 20 the coding key 26 situated in the temporary storage register 15 of the information transmitting terminal device 10 is deleted, and the same happens with the coding key 16 situated in the temporary storage register 25 of the information transmitting terminal device 20.

After finishing the call of the information transmitting terminal device 10, in the information transmitting terminal device 20 only its own decoding key 27 situated in the D-register 24 and the master coding key 41a situated in the C-register 23 remain. At the same time the information transmitting terminal device 10 only keeps its own decoding key 17 situated in the D-register 14 and the master coding key 41a situated in the C-register 13.

On the basis of describing the process it can be seen that in the course of establishing data forwarding the information transmitting terminal device 10, the information transmitting terminal device 20 and the central traffic co-ordinating unit 40 do not get in a position even for a moment when they have a coding-decoding key pair belonging together at the same time. So it is not possible for anyone of the users of the set of equipment to have access to the coding key 16 and the decoding key 17, or the coding key 26 and the decoding key 27 at the same time.

It is obvious that the central traffic co-ordinating unit 40 is able to store and administrate network addresses needed for network access, determined by the characteristics of the information forwarding network 40, and forward the addresses needed for establishing connection towards the information transmitting terminal devices 10 and 20.

In the interest of increasing security even more, it can also be solved that the central traffic co-ordinating unit 40 does not contain the master coding key 41a and the master decoding key 42a at the same time. Knowing only one member of the coding-decoding key pairs makes it impossible to decrypt encrypted messages.

List of references

10 information transmitting terminal device	11 storage partial unit
	12 ID-register
	12a device identifying signal
	13 C-register
	14 D-register
	15 temporary storage register
	16 coding key
	17 decoding key
	18 sender partial unit
	19 receiver partial unit
20 information transmitting terminal device	21 storage partial unit
	22 ID-register
	22a device identifying signal
	23 C-register
	24 D-register
	25 temporary storage register
	26 coding key
	27 decoding key
	28 sender partial unit
	29 receiver partial unit
30 information forwarding network	
40 central traffic co-ordinating unit	41 MC-register
	41a master coding key
	42 MD-register
	42a master decoding key
	43 memory unit
	43a base cell
	43b base cell

CLAIMS

1. Set of equipment according to the invention for secure direct information transfer over the Internet, which contains information transmitting terminal devices suitable for collaborating with an information forwarding network, taking part in the information traffic, the individual information transmitting terminal devices are equipped with a sender partial unit, a receiver partial unit and a storage partial unit comprising an ID-register containing a device identification signal, a C-register suitable for storing a coding key and a D-register suitable for storing a decoding key, where the C-register containing the coding key is in connection with the sender partial unit, and a coding key and a collaborating decoding key are allocated to the individual information transmitting terminal devices, the storage partial unit of each information transmitting terminal device is completed with one or more temporary storage registers for the temporary storage of the coding keys of other information transmitting terminal devices, while the information forwarding network is completed with at least one central traffic co-ordinating unit, the central traffic co-ordinating unit has an MD-register storing a master decoding key and a memory unit containing base cells for storing the coding keys belonging to the individual information transmitting terminal devices and a master coding key collaborating with the master decoding key is allocated to the central traffic co-ordinating unit, and the C-registers of the information transmitting terminal devices are provided with a master coding key collaborating with the master decoding key stored in the MD-register of the central traffic co-ordinating unit, **characterised by** that in the storage partial unit (11, 21) of the individual information transmitting terminal devices (10, 20) there is only information free from the given information transmitting terminal (10, 20) device's own coding key (16, 26), while only the coding key (26) of the other information transmitting terminal device (20) participating in the information exchange is temporarily stored in the temporary storage register (15) of the first information transmitting terminal device (10), and only the coding key (16) of the first information transmitting terminal device (10) participating in the information exchange is temporarily stored in the temporary storage register (25) of the other information transmitting terminal device (20), and so for the duration of the actual

information exchange the first information transmitting terminal device (10) and the other information transmitting terminal device (20) are directly linked to one another permitting data flow without the mediation of the central traffic co-ordinating unit (40).

2. Set of equipment as in claim 1, **characterised by** that the temporary storage registers (15, 25) of the information transmitting terminal devices (10, 20) are connected to the sender partial unit (18, 28).
3. Set of equipment as in claim 1 or 2, **characterised by** that the central traffic co-ordinating unit (40) is provided with an MC-register (41) storing a master coding key (41a).